

Feb 03, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)Single-family residence and garage located at N3184  
Evergreen Rd, Lake Geneva, WI 53147; the Black Infinite  
QX80 SUV bearing WI license plate number "ARW2153"  
located at N3184 Evergreen Rd, Lake Geneva, WI 53147;  
and the person of James BUSHEY (See Attachments)

Case No. 23 MJ 3

Matter No.: 2021R00255

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure  
of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before 2/17/2023 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to \_\_\_\_\_  
Honorable William E. Duffin  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 2/3/2023 at 1:56 PM

William E. Duffin

Judge's signature

City and state: Milwaukee, WI.

Honorable William E. Duffin, Magistrate Judge

Printed name and title

**Return**Case No.:  
23-MJ-3 772120-21-0084Date and time warrant executed:  
02/09/2023 0800 hoursCopy of warrant and inventory left with:  
James Bushey

Inventory made in the presence of :

ATF Special Agent Alex Erlien

Inventory of the property taken and name(s) of any person(s) seized:

The cell phone of James Bushey, extracted from that phone was call lists, contacts lists, text messages, photos, videos, applications, files, social media information, emails, and other electronic information associated with cell phone forensic images

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 03/01/2023

RICHARD CONNORS

Digitally signed by RICHARD  
CONNORS  
Date: 2023.03.01 11:04:27 -06'00'

*Executing officer's signature*

ATF Special Agent Richard Connors

*Printed name and title*

ATTACHMENT A  
Property and Person to Be Searched

- The single-family residence and garage located at N3184 Evergreen Rd, Lake Geneva, WI 53147. This residence is described as a two-story residence with green siding and an attached garage. The residence has a driveway that consists of both cement and brick, and to the south of the drive is a blue colored fire sign with “N3184” posted on it. The residence is located on the east side of Evergreen Road;
- Black Infinite QX80 SUV bearing WI license plate number “ARW2153” located at N3184 Evergreen Rd, Lake Geneva, WI 53147; and
- The person of James BUSHEY

ATTACHMENT B  
Particular Items to Be Seized

1. All records relating to violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal Import of Ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); 18 U.S.C. § 545 (Smuggling); and impersonating an officer or employee of the United States (18 U.S.C. § 912), those violations involving Darin DOWD, Jacob DOWD, Eli LAZAR, James BUSHEY and others and occurring after January 1, 2020, including:

- a. Records related to firearms, ammunition, firearm accessories, to include pistols, handguns, shotguns, rifles, machine guns, silences, NFA weapons, magazines;
- b. Records and information relating to a conspiracy to defraud the ATF and the government;
- c. Records relating to firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments
- d. Records relating to any ATF forms or firearm or ammunition licensing;
- e. Records and information relating to UFE firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments;
- f. Records related to the impersonation of law enforcement, including federal ATF agents;
- g. Records related to financial transactions and travel records for UFE owners, employees, and associates;
- h. Records and information relating to the e-mail and social media accounts connected to UFE, Darin DOWD, Jacob DOWD, James BUSHEY, and Eli LAZAR;
- i. Records and information relating to the identity or location of the suspects;

- j. Records and information relating to communications with Internet Protocol addresses;
- k. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- l. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- m. The contents of all emails associated with the account from 02/12/18 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses

associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- n. The contents of all instant messages associated with the account 02/12/18 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- o. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- p. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,

downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

- q. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- r. All records pertaining to the types of service used;
- s. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- t. Records related to all files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web



pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of James BUSHEY to the fingerprint scanner of the device; (2) hold a device found in front of the face of James BUSHEY and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.